REMARKS

Claims 23-41 are pending. Claim 25 is amended to address the rejection under 35 U.S.C. § 112, second paragraph. Claims 26 and 37 were amended solely to address antecedent basis issues. Claims 1-22 were previously canceled. Withdrawal of all outstanding rejections is respectfully requested.

Request for Interview Prior to Formal Action on Amendment

Applicants request an interview prior to formal action on this response. An "Applicant Initiated Interview Request Form" accompanies this response. Please contact Applicants' undersigned representative to schedule the interview.

Drawings

Fig. 2 was amended to add an inadvertently missing label "50." The element named "ActiveGuard™" is the security subsystem 50 described throughout the specification. Fig. 2 was further amended to label the network devices with the same labeling shown in Fig. 1. This amendment is supported by page 6, lines 28-30 of the specification that states that "[t]arget network 100 is shown having the same basic components as the network of the prior art shown in FIG. 1..." Accordingly, no new matter was added.

35 U.S.C. § 112, second paragraph, rejection

1. Claims 24 and 34

The Examiner asserts that the limitations of claims 24 and 34 are not disclosed in the specification. This is incorrect. The claimed first communication medium refers to secure link 54. Referring to Fig. 2, the secure link 54 is connected at one end to master system 60 and at the other end to the security subsystem 50 (labeled as"ActiveGuard™" in the originally filed version of Fig. 2). See, also, page 7, lines 24-25 of the present specification, that reads as follows:

> A similar secure link 54 is established as a virtual private network (VPN) tunnel between the security subsystem 50 and a master system 60 connected to a remote network 110.

The secure link 54 is not connected to any of the network devices 14, 18, 20 or 22. Accordingly, the limitations of claims 24 and 34 are believed to be properly disclosed in the specification.

2. Claim 25

The Examiner asserts that claim 25 is not enabled. Applicants disagree with this assertion, and believe that the text on page 8, line 27 through page 9, line 19 of the specification clearly supports this claim. Nonetheless, to advance prosecution of the patent application, claim 25 was amended to mirror the exact language provided on page 8, line 31 through page 9, line 6 of the specification, which reads as follows (underlining added for emphasis):

> Although information preferably flows both ways between master system 60 and security subsystem 50 in this embodiment, the master system in this embodiment does not take direction from the subsystem.

3. Claim 26

The Examiner asserts that claim 26 is not disclosed in the specification. In response, the claimed second communication medium is described on at least page 9, lines 17-19 of the specification, which reads as follows:

> Additionally, if the link 54 between master system 60 and security subsystem 50 is severed or compromised, instructions may be routable instead through secure links 55.

Even though the secure link 55 is established through an encrypted communication protocol, it is still a "communication medium" as broadly recited in claim 26. Claim 27 further defines when the secure link 55 is used and exactly matches the specification language highlighted above.

Prior Art Rejections

Claims 23, 28-29, 33 and 40-41 were rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by Emigh. This rejection is respectfully traversed.

The Emigh article discusses various security products and services, including NetRanger and IBM's Network Security Operations Center (NSOC). To assist in understanding the Emigh article, Applicants submit concurrently herewith a User's Guide for NetRanger, also cited on an accompanying Supplemental Information Disclosure Statement.

NetRanger includes three main components, namely, a NetRanger Sensor, a NetRanger Director, and a NetRanger Post Office. A sample configuration for these components is shown in Figure 1.3 of the User's Guide (page 1-4), attached hereto as an Appendix.

The NetRanger Sensor is a network appliance that uses a rules-based engine to distill large volumes of IP network traffic into meaningful security events, which it forwards to the NetRanger Director. The NetRanger Sensor can either capture network traffic directly from the network or receive it directly from a network device, such as a STK packet filter firewall. The NetRanger Sensor can also log security data, reset TCP sessions, and dynamically manage a router's access control system to shun intruders.

The NetRanger Director provides a centralized graphical interface for the management of security across a distributed network. It remotely monitors and manages the NetRanger Sensors.

The NetRanger Post Office is a communication infrastructure that allows Sensors and Directors to communicate with each other.

In the outstanding Office Action, the Examiner presumes that either the NetRanger Sensor is equivalent to the claimed security subsystem, or that the combination of the NetRanger Sensor and NetRanger Director is equivalent to the claimed security subsystem. Since it is unclear from the Examiner's rejection which analogy is being asserted, both will be addressed.

As clearly explained and illustrated in the NetRanger product manual, the NetRanger Sensor is just another device connected to a computer network and has the specific purpose of detecting and analyzing IP network traffic (i.e., traffic among and between devices on the network). The NetRanger Director remotely monitors and manages the NetRanger Sensors. Upon review of the NetRanger User's Guide, no description was located regarding the ability of

the NetRanger Sensor or NetRanger Director (or the combination thereof) to monitor activities of any devices on a network (as opposed to merely monitoring network traffic associated with the network device). Monitoring activities of at least some devices on a network is an explicitly recited function performed by a security subsystem in claim 23. Nor was any description located in the NetRanger User's Guide of the ability of the NetRanger Sensor or NetRanger Director to test the integrity of security-related functions of devices on a network that have security-related functions. This function is explicitly recited in claim 33 as being performed by the security subsystem.

In the outstanding Office Action, the Examiner also presumes that the claimed master system is equivalent to IBM's NSOC. However, nowhere does Emigh describe that the NSOC monitors the integrity of the NetRanger Sensor, NetRanger Director, or combination thereof. In fact, the only connection between the NSOC and NetRanger appears to be that the NSOC hosts the NetRanger Director (see lines 31-32).

On lines 37-46, Emigh makes the following statements regarding functions performed by IBM's NSOC:

IBM's NSOC	Applicants' remarks
Also, from Boulder, IBM will conduct weekly and monthly testing of network devices like Web Servers and name servers for "vulnerability," and will make remote configuration changes as needed…	This testing is not described as being connected in any manner to NetRanger, and thus is not part of a system having a security subsystem and a master system as set forth in the claims.
In addition to responding to any hacker attempts immediately, IBM will regularly issue written reports to customers as to the security status of their own networks, along with advisories from hacker watchdog groups like CERT and CEAC…	These reports and advisories are not described as being connected in any manner to NetRanger, and thus this text is not relevant to the pending claims.
Also, at the NSOC, IBM will consolidate NetRanger Director log files from multiple customers into a separate database for trend analysis, to uncover patterns in detected activities of hackers.	This consolidation does not relate in any manner whatsoever to monitoring the integrity of the NetRanger Sensor, NetRanger Director, or combination thereof.

Put simply, if the integrity of a NetRanger Sensor is compromised, there is no disclosure or suggestion in Emigh or in the NetRanger User's Guide that any entity such as the NSOC

would necessarily detect this fact or even has the capability of doing so. Accordingly, the NSOC does not monitor the integrity of any security subsystem, as recited in both claims 23 and 33.

Lines 28-32 of Emigh describe that NetRanger Sensors are "located at places on a corporate network," and that the NetRanger Director is used by IBM "at the NSOC." Thus, even though it is unclear from the Examiner's rejection which analogy of elements is being asserted, one logical interpretation of the Examiner's rejection is that the NetRanger Sensors are supposed to be equivalent to the claimed security subsystem and that the NetRanger Director is supposed to be equivalent to the claimed master system. However, even that analogy fails to disclose or suggest the claimed invention.

First, as discussed above, no description was located in the NetRanger User's Guide regarding the ability of the NetRanger Sensor to monitor activities of any devices on a network, which is a function recited in claim 23 as being performed by a security subsystem. Again, NetRanger is just another device connected to a computer network and has the specific purpose of detecting and analyzing IP network traffic (i.e., traffic among and between devices on the network). Nor was any description located in the NetRanger User's Guide regarding the ability of the NetRanger Sensor to test the integrity of security-related functions of devices on a network that have security-related functions, which is a function recited in claim 33 as being performed by the security subsystem.

Second, even though the NetRanger User's Guide describes that the NetRanger Director remotely monitors and manages the NetRanger Sensors, no description was located regarding the ability of the NetRanger Director to monitor the integrity of the NetRanger Sensor. The primary function described for the NetRanger Director is to receive and record alarms (e.g., policy violation alarms) from NetRanger Sensors. Put simply, if the integrity of a NetRanger Sensor is compromised, there is no disclosure or suggestion in Emigh or the NetRanger User's Guide that the NetRanger Director would necessarily detect this fact or even has the capability of doing so. Accordingly, the NetRanger Director does not monitor the integrity of any security subsystem, as recited in both claims 23 and 33.

2. Patentability of claims 23 and 33 over Emigh

For at least the reasons discussed above, Emigh fails to disclose or suggest the claimed combination of a security subsystem and a master system, and at least the following underlined limitations:

> 23. A security system for a computer network, the network having a plurality of devices connected thereto, the security system comprising:
> (a) a security subsystem connected to at least some of the devices in the network, the security subsystem configured to monitor activities of the at least some devices on the network and detect attacks on the at least some devices;
> (b) a master system which monitors the integrity of the security subsystem and registers information pertaining to attacks detected by the security subsystem; and
> (c) a first communication medium connected between the security subsystem and the master system, the master system monitoring the integrity of the security subsystem and receiving the information pertaining to the attacks through the first communication medium.
>
> 33. A security system for a computer network, the network having a plurality of devices connected thereto, at least some of the devices having security-related functions, the security system comprising:
> (a) a security subsystem associated with at least some of the devices in the network which tests the integrity of the security-related functions;
> (b) a master system which monitors the integrity of the security subsystem and receives and stores results of the integrity testing of the devices having security-related functions; and
> (c) a communication medium connected between the security subsystem and the master system, the master system monitoring the integrity of the security subsystem and receiving the results of the integrity testing of the devices having security-related functions through the first communication medium.

In view of the above remarks, claims 23 and 33 are believed to be patentable over Emigh.

3. Patentability of dependent claims 24-32 and 34-41

The dependent claims are believed to be patentable over the applied references for at least the reason that they are dependent upon allowable base claims and because they recite additional patentable elements and steps.

Conclusion

Insofar as the Examiner's rejections were fully addressed, the instant application is in condition for allowance. Issuance of a Notice of Allowability of all pending claims is therefore earnestly solicited.

Respectfully submitted,

MICHAEL HRABIK et al.

August 12, 2005 By: Anna Vishev
(Date)

ANNA VISHEV
Registration No. 45,018
SCHULTE ROTH & ZABEL LLP
919 Third Avenue
New York, NY 10022
Telephone: (212) 756-2000
Direct Dial: (212) 756-2167
Facsimile: (212) 593-5955
E-Mail: anna.vishev@srz.com

Enclosure (Fig. 2, Appendix)

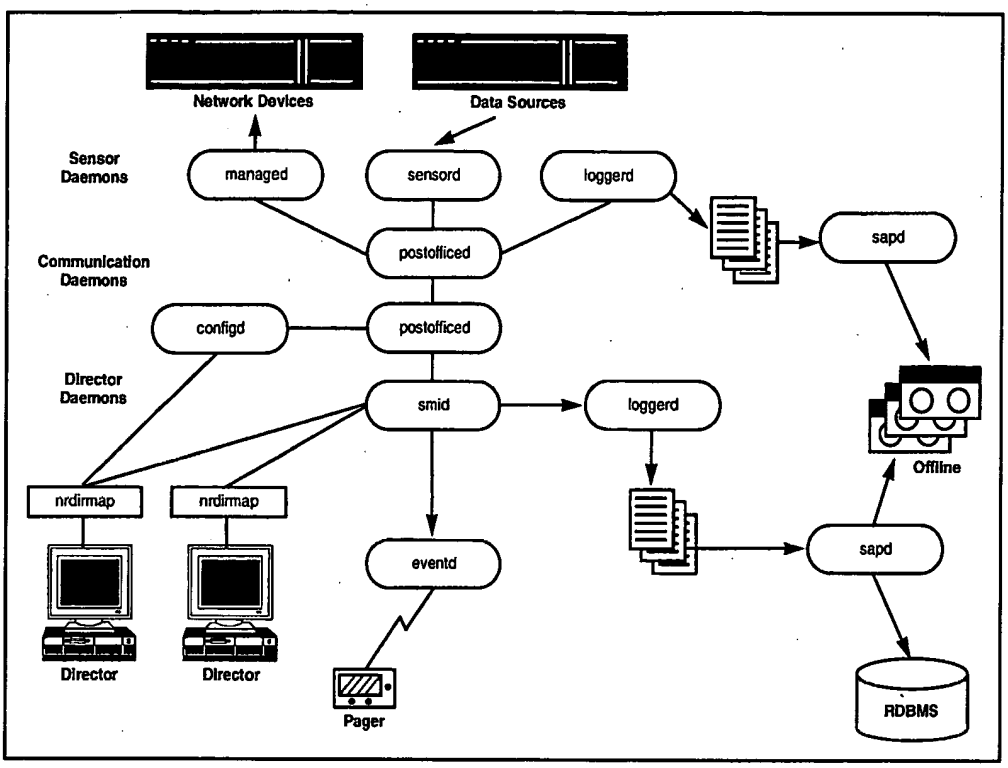

Figure 1.3: NetRanger 2.1.1 Architecture

The NetRanger Sensor

The **Sensor** handles real-time intrusion detection and device management. It uses a rules-based engine to distill large volumes of IP network traffic into meaningful events. A Sensor can either capture network traffic directly from the network or receive it from a network device, such as an STK packet filter firewall.

The **Packet Filtering Device** is a router or firewall residing on the network at a point of entry to other networks. The Sensor can reconfigure these devices on the fly to shun the source of an attack. Many of these devices can also serve as the data source for the Intrusion Detection subsystem. Device management is optional because there are places within networks where detection is all that is required—e.g., at connections between internal networks.

The Communication System

The **Post Office** subsystem provides the communication backbone for remote monitoring and management of the Sensor network device. All communication is supported by a proprietary, connection-based protocol that can switch between alternate routes to maintain the point-to-point connections specified in its routing tables. All messages are routed based on a three-part address that includes organization, host, and application identifiers.